http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 7 (5): 802-807, 2008
ISSN 1812-5638

Distributed Signature Scheme (DSS) Based on RSA

T. Pazynyuk, G.S. Oreku and J. Li
Department of Computer Science and Engineering, Harbin Institute of Technology,
150001, Xidazhi Street, 92 Nangang District, P.O. Box 750, Heilongjiang, China

Abstract: The present study proposes a set of security provisions for node to base station communication in wireless sensor networks. The Distributed Signature Scheme (DSS) is another important security service which will enables sensor nodes to communicate securely. A key-management scheme designed to satisfy both operational and security requirements of Distributed Sensor Networks (DSS) is presented. The scheme includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication capabilities. The presentation describes a secret distribution scheme for sensor networks that achieves automatic secret redistribution. The goal is to support the distribution of secret key among new nodes members joining the network without involving a trusted agent or intervention from the user. Present analysis indicates that, the proposed schemes have better features compared with previously presented methods. In particular the system is efficient, second, it guarantees automatic key distribution after initializations, third it does not need urgent for key distribution and in additional, it automatically interact nodes coalition.

Key words: Data aggregation, distributive asymmetric signature, security

INTRODUCTION

Wireless sensor networks have recently emerged as an important means to study and interact with the physical world. A sensor network typically consists of a large number of tiny sensor nodes and possibly a few powerful control nodes (also called base stations). Many protocols and algorithms (e.g., routing, localization) will not work in hostile environments without security protection (Liu and Ning, 2007).

The use of aggregation in WSN allows the increasing of efficiency and significantly survivability of sensor nodes. In this study many aspects of the wireless sensor network are being examined including security and efficient data aggregation (Deborah *et al*., 1999; Lingxuan and David, 2003; Samuel *et al*., 2002; Nisheeth *et al*., 2004; Huafei *et al*., 2004). For example, Base Station (BS) was used to define the integral characteristic of any part of WSN; and assign one of the nodes as aggregator for clear elaboration and understanding of this study. The node will gather the needed information from the area, calculate the aggregation functions (i.e., average, min, max) and transfer this value to the BS. By so doing this will facilitate the cut down of total transmission cost rather than with the use of aggregator. But, all in all there is a need of special and reliable aggregation algorithms when it comes to node failing fulfilling their tasks. e.g., when the adversary can capture the nodes and change their functionality or the aggregator is compromised and brings total destruction to its function, i.e., when aggregator is compromised and sends the wrong information to the BS. For solving this kind of problems, special cryptography procedures can be used (Schneier, 1996; Laurent and Gligor, 2002; Chan *et al*., 2003; Gura *et al*., 2004; Joengmin and Kim, 2004; Liu and Ning, 2005). Some of the solutions sited might allow BS to define incorrect aggregation result with high probability. And in this case the aggregation might be called reliable.

It's clear, that it's necessary to provide reliability requirements to transmit some extra data from aggregator to BS. In this case we argue that these data capacity (size) should be minimized with given reliability. In the existing reliability aggregation protocols at present, the size of extra data used is sufficiently high. This sets conditions and motivations for further interest in creating new reliable aggregation protocols, though it should be noted that creating special protocols for WSN also have some shortcomings; mainly being high number of keys to be kept by each sensor. However in providing reliable aggregation in WSN, the key management protocol issues should also be realized. The present solutions used for classical networks are unable to implement some of these options to WSN due to sensor's limitations and unfeasibility of using sensor's infrastructure.

Corresponding Author: Tamara Pazynyuk, Department of Computer Science and Engineering, Harbin Institute of Technology, 150001, Xidazhi Street, 92 Nangang District, P.O. Box 750, Heilongjiang, China

Talkless of lots of constraints when it comes to providing security services in sensor networks, it also turns out to be a very challenging task. With the same lane of creating reliability in data aggregation, we introduce our finding to solve the problem of scheme distribution for signing the accurate information within nodes participating in transmitting the final information to BS. Having this kind of mechanism will allow to substantially decreasing energy consumption by eliminating the transmission of fake packets within the sensor networks meanwhile enhance the accuracy of security.

In this study, we have shown Distributed Signature Scheme Design based on RSA. The scheme presents several advantages, i.e., secure provable mathematics and application efficiency, security properties which did not exist in previously schemes.

RELATED WORKS

Blakley and Shamir invented secret sharing schemes independently. In Blakley's scheme (1979), the intersection of m of n vector spaces yields a one-dimensional vector that corresponds to the secret. Theodore *et al.* (2002) scheme is one of several to catch a dealer that attempts to distribute invalid shares. Gennaro *et al.* (2008) present a verification of a signature using a regular public key and a standard verification procedure; hence the verifier of a signature does not need to be aware of the form (centralized or distributed) in which the signature was generated, or who were the parties involved, nor does the signature increase in size as a function of the number of signers.

Our DSS scheme differs from previous VSS schemes in that it achieves automatic secret redistribution without the use of agent's. Also, unlike in VSS schemes, with signature setting actions node members can associate independently in present DSS. However secret key distribution protocol is un-interactive and doesn't require agent participation after scheme initialization.

A proactive RSA scheme for large-scale ad hoc networks proposed by Haiyun *et al.* (2004). In their scheme, every node in ad hoc networks has a secret share of the secret key (the private key d). Nodes within one-hop distance jointly perform issuing certificates and refreshing their secret shares. The scheme is efficient. Unfortunately, the scheme has proved faulty (Maithili *et al.*, 2007; Stanislaw *et al.*, 2004). All the previous schemes (Blakely, 1979; Laurent and Gligor, 2002; Chan *et al.*, 2003) can be considered as special instances in this framework.

Rui-Shan and Ke-Fei (2007) have presented a new proactive RSA scheme for ad hoc networks, which includes four protocols, the initial key distribution protocol, the share refreshing protocol, the share distribution protocol and the signature generation protocol. Their study mainly based on use of efficient proactive threshold RSA signature scheme. The initial key distribution protocol is used to distribute the initial secret shares to 2t+1 R nodes. Before distributing the secret key, they assume that a setup process has been carried out in which the RSA key generation took place and the RSA key pair has been computed where by in present study the agent is used to initialize the distributed signature's scheme and hence, all the remaining process is independently operated.

By instantiating the components in above frameworks, we further develop our distributed signature scheme DSS based on RSA with automatic signature setting procedure which provide coalition between (nodes) members, system with self-organizing property, i.e., the agent is not involved after initialization and during secret distribution process.

RSA BASED DISTRIBUTED SIGNATURE SCHEME

Using only symmetric algorithms with authentication of sending data from sensors to BS have some disadvantages as well e.g., only BS might be able to authenticate final report sent by aggregator towards BS. This means, there is a chance of any compromised node to be sent into network and by chance this fake packets might only be detected or thrown off by BS at the end point. With accomplishment of the all process the sensor node's resources would have been consumed for sending the fake packets.

For sensor networks with more powerful nodes, solving this kind of problem can be based on the use of distributive asymmetric signature. This sort of signature assumes the distribution of digital signature of asymmetric algorithm secret key by threshold circuit (scheme) key distributed between the all scheme members. Also this scheme assumes the presence of protocol which allows coalition from a given number of members to compute digital signature for given message in distributed manner. Regarding the fake packets filtering task in WSN the digital asymmetric signature algorithm can be used as follows:

Agent chooses and distributes digital signature's chosen algorithm secret key between all the sensors and hence, all the sensors are initialized by public key. For sending the aggregation result to BS, the results are signed by given number of sensors using signature

distribution protocol. Furthermore each sensor, retransmitting data packet by using public key, can check the packet by itself and if the signature does not surpass the checking, it is automatically ejected from the network. For system to work effectively, distributed signature protocols should have some properties.

- The ability of independently correlate the sensors members working during signature signing setting. This property enables the restarting of signature signing setting protocol with changing of sensors members within the network. Also it reduces signature setting delay
- Self-organizing capability, i.e., after initialization of steps the system should be able to work automatically. With the missing of this important property to many of the systems today we introduce the approach of automatic interactiveness distribution procedure to this study also

For the interactive protocol assuming the process of data exchange between working (nodes) members is an essential shortcoming due to limited traffic capacity existing in today's many WSN, additionally it increases energy consumption, whereas the synchronization in sensors networking is necessary. The schemes which can guarantee security is suitable for sensor network security at present.

Distributed Signature Scheme with two described properties earlier can easily be established based on El-Gammal or DSS digital signature (Elgamal, 1985). Unlike these digital signatures, based on RSA digital signature, no existing study, to the best of our knowledge, has addressed the issue of developing distributed signatures schemes with above-listed properties at the moment. However, RSA digital signature has one important property which does not exist in El-Gammal and DSS schemes. For RSA signature, the signature checking procedure is substantially accelerated if public key value is correctly chosen. This characteristic provides significant advantage for RSA distributed signature use in WSN.

Scheme assumptions: The system model assumes that we have n nodes and one malicious node (note that for this example we will use only one malicious node though in really application our approach should be able to withstand up to t-1 compromised nodes). Also the system has a trusted agent which initializes the scheme. For this case agent chooses RSA secret key and distribute this key safely between the nodes providing (t, n)-threshold circuit. After this initialization the participation of trusted agent is not needed. Assuming that malicious can compromise s<t of nodes and since malicious is able to break the multiple signature scheme, he could execute attack by chosen message (we call it chosen-message attack, CMA); therefore he could request any of n nodes members to invoke signature protocol for any chosen message. In this situation malicious aim is either tamper message signature which he/she did sign or disrupt a wrong message signed by another member.

Present distributed signature scheme RSA should be successfully able to resist against malicious actions from assumption above at the same time satisfy the following properties:

- Signature setting procedure should automatically provide coalition action between nodes members
- System should have self-organizing property, i.e., the agent should not be involved after initialization
- Procedure of secret projection distribution without agent should be un-interactive

In existing study based on distributed RSA signature there are three main approaches as far as RSA based secret key distribution is concerned. In the first approach, the secret key d is distributed according to Shamir secret scheme separation over $Z_{\phi(N)}$ ring (or $Z_{\lambda(N)}$) (Shamir, 1979), where, $Z_{\phi(N)}$ (or $Z_{\lambda(N)}$) advancement are not presented in most of literatures to the best of our knowledge. This fact of lack of information about $Z_{\phi(N)}$ (or $Z_{\lambda(N)}$) prevents many researchers from simply extending the establishment of system working without trusted agent.

In the second approach, the level in secret scheme separation has been added. Firstly, the secret is distributed between n nodes additively and then every received projection is distributed by threshold circuit. Such schemes are interactive and are unable to work without agent.

In the third approach, there is secret key d separation over the known ring Z_N instead of $Z_{\phi(N)}$ (or $Z_{\lambda(N)}$). But this kind of separation brings vulnerability to distributed scheme. Moreover this approach doesn't assume independent working members nodes coalition during signature setting. Thus, each of approaches noticed above have some functional limitation and do not employ at least one of the properties formulated earlier.

The presented secret separation scheme incorporates components of distributed signature scheme. In particular, Shamir scheme can be used for distributed RSA based signature scheme in our approach as well. In Shamir scheme there is polynomial function:

$$f(x) = f_0 + f_1 x + ... + f_{t-1} x^{t-1} \ \text{mod} P \quad (1)$$

Where:
$f_0 = S$ = Secret
$f_1,...f_{t-1}$ = Random values
P = Prime No.

Each member of protocol gets the secret projection in ss = f(id) form, where, id is member ID. Any coalition K of t members could restore (recover) the secret $f_0 = f(0)$ using lagrange interpolation:

$$f(0) = \sum_{u \in K} ss_u l_u(0) (\text{mod} P) \quad (2)$$

where, $l_u(x)$ are Lagrange coefficients.

For Shamir scheme to be used in distributed RSA signature, it's necessary to choose the secret S and module P. For distributed RSA signature secret key d is the secret. Relatively to module P there are two ways, either make it public, e.g., P = N or make it secret, i.e., $P = \phi(N)$ or $P = \lambda(N)$. If P is known (e.g., module RSA N), that brings information leakage and interdependency of coalition members actions during the distribution of signature setting procedure running. If P is a secret value (e.g., $P = \lambda(N)$ or $P = \phi(N)$, that gives the system possibility of being not self-organized according to the next statement.

Statement 1: In case of using module P and this P module is unknown to members, then it's necessary to have trusted agent for secure project distribution to new member.

It is necessary to ignore the use of module P approach to eliminate disadvantaged listed earlier. However, projection distribution procedure without agent remains interactive. In addition, abandonment of P increases projections size eventually to complexity of signature setting. It's easy to get higher estimation of secret R projection size by using:

$$R \le \log(N) + (t-1)k + 1 \quad (3)$$

Where:
N = RSA module
t = Coalition size
k = User ID length

For example, for user ID length k = 48 bit and coalition size t = 10, projection size R will not be over log(N)+ 48(t-1)+1 ≈1500 bit which means there is an increase of signature setting complexity of approximately 1.5 times.

OUR APPROACH ON SCHEME ESTABLISHMENT

It was proposed that to modify secret distribution scheme by getting rid of interaction in distribution procedure of new projection without agent (statement 1) and reduce the size of secret projection signing. We put into consideration prime number Q>max (id_i). We estimate the secret projection as follow:

$$f(x,y) = \sum_{i=0}^{t-1} \sum_{j=0}^{t-1} f_{i,j} (x^i \text{mod} Q)(y^j \text{mod} Q) \quad (4)$$

It's impossible to use La Grange interpolation with such kind of secret distribution function setting. Instead, it's essential to solve the combined linear equations.

For secret recovering, each of coalition member node u calculate its function value on point x = 0 getting

$$f(0, id_u) = f_0 + f_1 (y \text{mod} Q) + ... + f_t (y^t \text{mod} Q) \quad (5)$$

in $y = id_u$ and $f_0 = f_{0,0}$. Having t-values of given function, secret can be recovered by solving the following combined equations:

$$\begin{bmatrix} f(x_{i_1}) \\ f(x_{i_2}) \\ ... \\ f(x_{i_t}) \end{bmatrix} = G \begin{bmatrix} f_0 \\ f_1 \\ ... \\ f_{t-1} \end{bmatrix}$$

Where:

$$G = \begin{bmatrix} (x_{i_1})^0 \text{mod} Q & (x_{i_1})^1 \text{mod} Q & ... & (x_{i_1})^{t-1} \text{mod} Q \\ (x_{i_2})^0 \text{mod} Q & (x_{i_2})^1 \text{mod} Q & ... & (x_{i_2})^{t-1} \text{mod} Q \\ & & ... & \\ (x_{i_t})^0 \text{mod} Q & (x_{i_t})^1 \text{mod} Q & ... & (x_{i_t})^{t-1} \text{mod} Q \end{bmatrix} \quad (6)$$

Each coalition member calculates its function value in $x = id_{new}$ getting

$$f(id_{new}, id_u) = s_{new}(id_u) = s_0 + s_1 (y \text{mod} Q) + ... + s_{t-1} (y^{t-1} \text{mod} Q) \quad (7)$$

in point $x = id_n$ for projection to be distributed to new members without agent. Secret projection ($s_0,...s_1$, s_{t-1}) for new user can be calculated from the following combined equations:

$$\begin{bmatrix} s_{new}(x_{i_1}) \\ s_{new}(x_{i_2}) \\ ... \\ s_{new}(x_{i_t}) \end{bmatrix} = \begin{bmatrix} s_0 \\ s_1 \\ ... \\ s_{t-1} \end{bmatrix} \quad (8)$$

The following statement is true for proposed secret distribution scheme according to statement number 2.

Statement 2: For modified secret separation scheme it's true that:

- Scheme has threshold and it is safe
- The procedure of projection distribution in scheme is un-interactive and doesn't request agent participation
- The procedure of projection distribution in scheme is safe
- Size of projection part used in scheme signing is bounded above by log(N)+k+t

New RSA based distributed scheme signature based on proposed modified secret separation scheme includes three steps.

Scheme initialization: Agent generates the prime number Q>max(id_i).

- Agent generates public RSA key N = pq and e>Q, where, e is prime number. Then agent generates secret key d as following:

  $ed = 1 \bmod \Phi(N)$

- Agent generates function

$$f(x,y) = \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} f_{i,j}(x^i \bmod Q)(y^j \bmod Q) \quad (9)$$

where, $f_{0,0}$ = d and coefficients $f_{ij} \in Z_N$ was randomly chosen with $f_{i,j} = f_{j,i}$ condition.

Each node u gets the function $s_u(x) = f(x, id_u)$ in the competence of secret key projection.

Distributive signature setting: The coalition K of t members is chosen. Each coalition member calculates partial signature by the formula:

$$S_u(m) = m^{s_u(0)} \bmod N$$

where, m is hash-function value of signing message, u∈k.

- After getting t partial signatures, signature's collector makes the matrix G for coalition K members and reverses it over the rational number field
- Signature collector calculates, $G' = \lambda G^{-1}$ where, λ is the least common multiple of all elements of matrix G^{-1}. Then signature collector calculates

$$S'(m) = (\prod_{j=1}^{t}(S_{u_j}(m))^{g'_{1j}}) \bmod N \quad (10)$$

- Using extended Euclid algorithm, collector finds such x, y as $x\lambda+ye = 1$
- Calculate the signature as:

$$S(m) = ((S'(m))^x m^y) \bmod N \quad (11)$$

Key projection distribution to new user: For getting secret key projection the new node u has to find coalition K from t as already initialized nodes and report them to its own id_{new}.

- Every coalition member u calculate its own function value with $x = id_{new}$, getting

$$f(id_{new}, id_u) = s_{new}(id_u) = s_0 + s_1(y \bmod Q) + ... + s_{t-1}(y^{t-1} \bmod Q) \quad (12)$$

in $y = id_u$

- The new node finds its secret projection $(s_0,...s_1, s_{t-1})$ from combined equations:

$$\begin{bmatrix} s_{new}(x_{i_1}) \\ s_{new}(x_{i_2}) \\ . \\ s_{new}(x_{i_k}) \end{bmatrix} = G \begin{bmatrix} s_0 \\ s_1 \\ . \\ s_{t-1} \end{bmatrix} \quad (13)$$

Thus, secret key projection distribution to a new node does not request the agent participation and it is not interactive.

For proposed scheme it can be seen that it allows generating correct RSA based signature and the next statement is true.

Statement 3: Proposed distributed signing scheme provides high security guarantee and even safer as RSA.

CONCLUSIONS

Here, presented a new key management scheme for large scale Distributed Sensor Networks (DSS). All such schemes must be extremely simple given the sensor-node computation and communication limitations. Our approach is also scalable and flexible with independent member nodes behavior, signature signing setting and un-interactive projection distribution protocol secret key with no agent participation.

The proposed distributed signature scheme unlike existing schemes has the following advantages:

- With signature setting actions node members can associate independently
- Secret key distribution protocol is un-interactive and doesn't require agent participation after scheme initialization

As one of the possible future directions, we observed that sensor nodes have low mobility in many applications. Thus it may be desirable to develop location-based schemes so that the nodes can directly establish a signature setting automatically.

REFERENCES

Blakely, R.G., 1979. Safeguarding cryptographic keys. Proceeding 1979 National Computer Conference, June 4-7, AFIPS Press, New York, pp: 313-317.

Chan, H., P. Adrian and S. Dawn, 2003. Random key predistribution schemes for sensor networks. IEEE Symposium on Research in Security and Privacy, May 11-14, IEEE Computer Society, Washington, DC., pp: 197-213.

Deborah, E., G. Ramesh, H. John and S. Kumar, 1999. Next century challenges: Scalable coordination in sensor networks. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom '99, August 15-19, ACM, Seattle, Washington, United States, New York, pp: 263-270.

Elgamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory, 31: 469-472.

Gennaro, R., R. Halevi, R. Krawczyk and T. Rabin, 2008. IBM, T.J. Watson Research Center to be Presented at Eurocrypt 2008. Springer Berlin, April, pp: 88-107.

Gura, N., A. Patel, A. Wander, H. Eberle and C.S. Sheueling, 2004. Comparing elliptic curve cryptography and RSA on 8-bit cpus. Workshop on Cryptographic Hardware and Embedded Systems, LNCS., 3156, August, Springer Berlin/Heidelberg, pp: 119-132.

Haiyun, L., K. Jiejun, Z. Petros, L. Songwu and Z. Lixia, 2004. URSA: Ubiquitous and robust access control for mobile ad hoc networks. IEEE/ACM Trans. Networking, 12: 1049-1063.

Huafei, Z., B. Feng and R.H. Deng, 2004. Computing of trust in wireless networks. Proceedings of 60th IEEE Vehicular Technology Conference, September 26-29, Los Angles, California, pp: 2621-2624.

Joengmin, H. and Y. Kim, 2004. Revisiting random key pre-distribution schemes for wireless sensor networks. Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks, (SASN '04), ACM Press, New York, USA., pp: 43-52.

Laurent, E. and V.D. Gligor, 2002. A key-management scheme for distributed sensor networks. Proceedings of the 9th ACM Conference on Computer and Communications Security, (CCS' 02), ACM Press, Washington, DC. USA., pp: 41-47.

Lingxuan, H. and E. David, 2003. Secure aggregation for wireless networks. Proceedings of the 2003 Symposium on Applications and the Internet Workshops, (SAINT'03) IEEE Computer Society, pp: 384-394.

Liu, D. and P. Ning, 2005. Establishing pairwise keys in distributed sensor networks. ACM Trans. Inform. Syst. Security, 8: 41-77.

Liu, D. and P. Ning, 2007. Security for Wireless Sensor Networks (Advances in Information Security). 1st Edn., Springer-Verlag, New York, ISBN: 978-0-387-32723-5 .

Maithili, N., T. Gene and H.Y. Jeong, 2007. On the utility of distributed cryptography in P2P and MANETs: the case of membership control. Computer Networks. Int. J. Comp. Telecommun. Networking, 51: 3632-3649.

Nisheeth, S., B. Chiranjeeb, A. Divyakant and S. Subhash, 2004. Medians and beyond: New aggregation techniques for sensor networks. Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, (SenSys '04), ACM Press, New York, USA., pp: 239-249.

Rui-Shan, Z. and C. Ke-Fei, 2007. An efficient proactive RSA scheme for large-scale ad hoc networks. J. Shanghai Univ., 11: 64-67.

Samuel, M., J.F. Michael, M.H. Joseph and H. Wei, 2002. Tag: A tiny aggregation service for ad-hoc sensor networks. OSDI '02: Proceedings of the 5th symposium on Operating systems design and implementation, December 9-11, Boston, Massachusetts, pp: 131-146.

Schneier, B., 1996. Applied Cryptography. 2nd Edn., John Wiley and Sons, Australia, ISBN 0-471-11709-9 .

Shamir, A., 1979. How to share a secret. Commun. ACM, 22: 612-613.

Stanislaw, J., S. Nitesh and H.Y. Jeong, 2004. An attack on the proactive RSA signature scheme in the URSA Ad Hoc network access control protocol. ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), October 25, Washington, DC. USA., pp: 1-9.

Theodore, M.W., W. Chenxi and M.W. Jeannette, 2002. Verifiable secret redistribution for archive systems. Proceedings of the 1st International IEEE Security in Storage Workshop, (PISSW '02) IEEE Computer Society Washington, DC, USA., pp: 94-105.